Ludwig-Maximilans-
Universität München
Dr. Pascal Reisert

Wintersemester 2018/2019
Übungsblatt 9
12. Dezember 2018

Übungen zur Kryptographie
Lösung

Aufgabe 33

a) Für eine Primitivwurzel und $p > 3$ ist $g^2 \neq 1$ und $\left(\frac{g}{p}\right) = -1$, denn aus $g = b^k \Rightarrow g^{(p-1)/2} = b^{p-1} = 1$.
Angenommen $g^k = 1, k \neq 2$, dann gilt $k|p-1 \Rightarrow k|2q \Rightarrow k = q$ oder $k = 2q$. Ist $k = q$, also ungerade, so ist $1 = \left(\frac{g^q}{p}\right) \neq (-1)^q = -1$ ein Widerspruch. Alternativ folgt auch aus $g^q \bmod p = \left(\frac{g}{p}\right) = -1$ bereits $k = 2q$.

b) Es ist $2^2 \neq 1$ für $p > 3$. Ist nun $q = 1 \bmod 4$, dann ist $\left(\frac{2}{p}\right) = (-1)^{4q(q+1)/8}$ und $\frac{q(q+1)}{2} = 1 \bmod 2$. Nach Teil a) ist 2 eine Primitivwurzel.

Aufgabe 34

a) Es gilt $g^{p-1} = 1, g^{\frac{p-1}{2}} \neq 1$ und da $x^2 = 1$ die Lösungen $-1, 1$ hat folgt, $g^{\frac{p-1}{2}} = -1$. Es folgt $\log_g(-1) = \frac{p-1}{2}$.

b) $\left(\frac{x}{p}\right) = 1 \Leftrightarrow \exists q : q^2 = x \bmod p \Leftrightarrow \exists 0 \leq j < p-1 : g^{2j} = x \bmod p \Leftrightarrow \exists 0 \leq j < p-1 : 2j = \log_g(x)$.

c) Sei h Primitivwurzel, also $h^j = g$ für ein $0 \leq j < p-1$. Es folgt $h = g^{\log_g(h)} = h^{j \log_g(h)} \Leftrightarrow p-1 | j \log_g(h) - 1 \Leftrightarrow \exists k : 1 = j \log_g(h) + (-k)(p-1) \Rightarrow \gcd(\log_g(h), p-1) = 1$. Andererseits folgt aus $1 + k(p-1) = j \log_g(h)$ bereits $h^j = g^{j \log_g(h)} = g^{1+k(p-1)} = g$. Dies zeigt insbesondere auch $j = \log_h(g)$ und damit $\log_g(h) \log_h(g) \equiv 1 \bmod (p-1)$.
Alternativ ist $h = g^{\log_g(h)}$ für eine Primitivwurzel g, also $\operatorname{ord}(h) = \frac{\operatorname{ord}(g)}{\gcd(\operatorname{ord}(g), \log_g(h))}$.[1] Es ist $\operatorname{ord}(h) = \operatorname{ord}(g)$ genau dann, wenn $\gcd(\operatorname{ord}(g), \log_g(h)) = 1$, also $\log_g(h)$ invertierbar modulo $\operatorname{ord}(g) = p-1$.
Für ein beliebiges $x \in \mathbb{F}_p^*$ ist $x = g^{\log_g(x)} = h^{\log_h(g) \log_g(x)}$ und damit $\log_h(x) = \log_h(g) \log_h(x) \bmod (p-1)$.

Aufgabe 35

a) Wir haben $\mathbb{Z}/40 \simeq \mathbb{Z}/5 \times \mathbb{Z}/8$. Primteiler sind 2 und 5. Wir berechnen $6^3 \cdot (-5) \bmod 41 = 6 \cdot 25 = 27 \neq 1$ und $6^{20} = (-14)^4 = 196^2 = 32^2 = (-9)^2 = 81 = -1$. Damit ist $g = 6$ eine Primitivwurzel.
Wir berechnen $m/2^3 = 5$ und $m/5 = 8$ sowie $\lambda_5 = 2 \bmod 5$ und $\lambda_8 = -3 \bmod 8$. Wir

[1] Offensichtlich gilt $h^j = g^{j \log_g(h)} = 1 \Leftrightarrow \exists k : j \log_g(h) = k \operatorname{ord}(g) \Leftrightarrow \exists k : j \frac{\log_g(h)}{\gcd(\operatorname{ord}(g), \log_g(h))} = k \frac{\operatorname{ord}(g)}{\gcd(\operatorname{ord}(g), \log_g(h))} \Rightarrow \frac{\operatorname{ord}(g)}{\gcd(\operatorname{ord}(g), \log_g(h))} \mid j$.

berechnen $g_5 = g^8 = 6^8 \bmod 41 = (-5)^4 = (-16)^2 = 10$ und $g_8 = 6^5 \bmod 41 = -14$ sowie $x_5 = 2^8 \bmod 41 = 10$ und $x_8 = 2^5 \bmod 41 = -9$. Dann gilt $g_5 = x_5$ und $g_8^2 = 196 = 32 = -9 = x_8$. Somit ist $\log_6(2) = \lambda_5 \cdot 8 + 2\lambda_8 \cdot 5 = 16 - 30 \bmod 40 = 26$.
Alternativ kann man die Berechnungen für 2^8 auf Berechnungen modulo 2 zurückführen. Wir erhalten $g_8 = -14$ und berechnen $g_8^{2^{3-1}} = g_8^4 = (-9)^2 = -1 \bmod 41$ als erzeugendes Element von $G(q^k) = \{x \in G : x^{q^k} = 1\}, q^k = 2$ und $x_8^4 = 1 \bmod 41$. Also $\nu_1 = 0$. Im zweiten Schritt ist $g_8^2 = -9$ und $x_8^2 = -1$. Weiter bestimmen wir $y' = (-9)^2 \cdot (-14)^{-2 \cdot 0} = -1, g' = g_8^4 = -1$ und $\mu_1 = 1$ und somit $\nu_2 = \nu_1 + 2^1 \cdot \mu_1 = 2$. Es ist wie erwartet $x_8^2 = g_8^4$. Im dritten Schritt wiederholen wir das Vorgehen. Jetzt ist $y' = (-9) \cdot (-14)^{-\nu_2} = -1$, also $\mu_2 = 1$. D.h. es ist $\nu_3 = 2$ und $\log_{-14}(-9) = 2$. Wie zuvor erhalten wir $\lambda_5 \cdot 8 + \nu_3 \cdot \lambda_8 \cdot 5 = 26 \bmod 40$.

b) Mit Hilfe des Computers berechnen wir für die beiden Primteiler 2 und 13:
$a := 6^{2^{1000}} \neq 1$ und $b := 6^{13 \cdot 2^{999}} \neq 1$,

```
a = 138_31015_44673_75507_94717_74923_08637_45043_94000_44998_
73227_47428_44067_19045_58669_62830_52240_85167_91143_63099_12029_
92082_24228_45671_98649_86535_58035_67642_50531_49568_97001_57068_
05759_65349_56867_20376_47708_94553_45501_14103_96261_04380_75931_
79628_68893_02502_59952_02645_46689_89431_26898_34022_47521_81083_
80038_58231_09276_58480_02061_38730_25148

b = 139_29611_89342_14751_72329_52563_77800_23537_29826_25521_
71936_89676_87550_48814_56366_46241_69592_41157_89246_04046_15565_
87307_47928_19090_87274_32888_71400_00825_66779_95084_71081_47245_
11493_81072_71500_28104_73969_86581_08248_44413_40436_79896_04174_
78656_52364_76183_97826_91520_71299_00181_78894_25554_20992_50481_
79585_58781_14841_17028_88367_36849_01888
b = -1
```

Damit ist $g = 6$ eine Primitivwurzel.

Wir berechnen mit dem Computer $\log_6(2)$ zu

```
7_62724_52035_80263_43730_28216_17723_96608_45392_34057_14228_32648_
32315_60570_36412_60132_64796_98010_14813_05843_56574_36579_65266_75821_
75178_40329_77925_96889_92720_06451_65960_98316_20345_10332_76660_14368_
21032_70308_72717_97399_46415_27721_45868_74142_43006_39227_46124_65380_
80833_65360_61953_40154_31007_91432_77287_08418_28552_82509_26742_85525_
17584
```

Aufgabe 36

Mittels Pohlig-Hellmann Reduktion können wir $\alpha = 98$ und $\beta = 1654$ bestimmen - also $K = 6595$. Für den ersten Schritt erhalten wir $Z_1 = 6595 = (1100111000011)_2$ also $z_1 = (10011100)_2$. Weiter ist $(D8)_{16} = (11011000)_2$, also $z_1 \oplus D8 = (1000100)_2 = (44)_{16} = „D“$.
Allgemein erhalten wir

```
CC:=$D815_14BC_266E_6D2A_1BA4_3064_0F1C_4991_75F3_4C31_7A3E_
82F3_4DEC_7910_7610_8415_EC57_3728_82F2_A88F_30C9_C683;
```

```
function bytefolge(K,N:integer);
external
CC:byte_string;
var
k,j,z,m:integer;
bb,dd:byte_string[44];
begin
for k:=1 to 44 do;
m:=K**k mod N;
z:=0;
for j:=4 to 11 do;
z:=bit_test(m,j)*2**(j-4)+z;
end;
bb[k-1]:=z;
end;
dd:=mem_xor(bb,CC);
return string(dd);
end.
```

erhalten wir

```
Die Klausur findet am 15. Februar 2019 statt
```